EasyChair Preprint

№ 9050

A Comprehensive Study on Cyber Legislation in G20 Countries

Nisarg Mehta, Priyansh Sanghavi, Manish Paliwal and Madhu Shukla

October 18, 2022

A Comprehensive Study on Cyber Legislation in G20 Countries

Nisarg Mehta[1][0000−0002−8978−9399], Priyansh Sanghavi[1], Manish Paliwal[1][0000−0002−5756−4881], and Madhu Shukla[2]

[1] School of Technology, Pandit Deendayal Energy University, Gandhinagar, Gujarat, India, 382007
[2] Marwadi University, Rajkot, Gujarat, India, 360003
Corresponding Author: Manish Paliwal

Abstract. Cyberlaw, often known as Internet law, is a branch of the judicial framework concerned with the legality of internet information technology. It governs the digital transmission of information, shopping-portal applications, and information security. It is associated with justice informatics and electronic components like systems, software, and hardware. This article covers various topics, including the existence and appropriateness of the open Internet, free expression, and online privacy. The standards contribute to a significant decrease in the number of people engaging in asymmetric warfare and also help to restrict their participation by safeguarding illegal access to information, free speech connected to Internet usage, personal space, information exchange, e - email domains, intangible assets, machinery, and web services, which include data storage devices. As internet traffic increases, so does the number of legal challenges worldwide. Because internet laws differ from one nation to another, reprisal can range from bedframes to jail, and police agencies can be hard to implement. Cyberlaw protects persons who utilize the Internet or operate an online company. Internet users need to grasp their country's local community and cyber legislation to identify whether behaviors are allowed or prohibited on the network. They can also keep us from engaging in illegal activities.

Keywords: Cyber Security · Cyber Law · Cyber Crime · Privacy

1 Introduction

A computer is a configurable machine that normally stores and processes information according to the user's instructions. In most cases, the user provides these instructions. The proliferation of the Internet and other virtual worlds has made it simpler and more convenient than ever before to transmit data and information across a variety of networks. The internet is used for a broad variety of applications, including as a platform for commerce and financial transactions. The vast majority of people who use the internet have some prior experience with computers, whether for personal or professional reasons. As a direct result of this, administrators are growing more concerned about vulnerabilities that

have not been fixed. Because of this, a new phenomenon is known as “Cyber Crimes" has surfaced. As a result, computer crimes, also known as cybercrimes, are defined as offences perpetrated with the assistance of a computer system or network and often take place in cyberspace, most notably on the Internet. Cyberattacks, in their most basic definition, cyberattacks are conducted via the use of the communications or technical infrastructure of the internet. A cybercriminal may exploit a device to get access to private information belonging to a user, sensitive information belonging to the firm, or secret government papers, or they may do so to delete the information. The illegal sale of private information or data via the internet is an example of a sort of cybercrime. Criminals that participate in such actions are sometimes referred to as “hackers," which is a term that describes this sort of offender. As a consequence of this, cybercrime is also often referred to as e-crime, computer-related crime, high-tech crime, online fraud, and new-age crime [43].

Cybercrime has become such a problem in today’s world that it is wreaking havoc on people, corporations, and even the government. Many different legal requirements have previously been enacted to address the internet-related crimes that have occurred. The term “Cyber Law" has been disseminated ever the whole globe to encompass that part of the legal system that deals with matters about cyberspace and law, such as concerns with online privacy and safety, among other topics. To put this another way, cyber law might be described as the laws and regulations that regulate cyberspace cyberattacks, digital and electronic signatures, data security and privacy, and other concerns that are addressed by cyber law[43].

2 Literature Review

2.1 Argentina

The E-Signature Law, the Digital Argentina Law, the Telecommunication Law, and the Personal Data Protection Legislation are some of the laws that make up Argentina’s cybersecurity system. Other laws include the Digital Argentina Law and the Telecommunication Law, the Broadband Service Law, and the Cyberwarfare Law. It is vital to note that both civilian and military institutions in Argentina are involved in the cybersecurity field. The Defense Ministry, as well as the National Cyber Security Directorate, are the two agencies competing in this field. In addition to this, a National Cyber Security Working Group has been created (ICIC Cert). However, the sector of cyber security does not have any publicly published national standards or certification systems. The argument suggests that Latin American nations that have higher levels of democracy may have less stringent cybersecurity regulations[37].

2.2 Australia

The computer crime Amendment Act Bill 2011 (the Bill) was adopted by the Australian Parliament. The Bill alters the Telecommunication (Unauthorized

Table 1. Categorization of Laws in Argentina

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Civil and Commercial Code of the Nation (Spanish)	2014	They have significant growth potential.	They have a less efficient Organizational Measurement.	91
Data Security and Privacy Regulations	Constitution of the Argentine Nation, Law No. 24,430, Enacted on December 15, 1994 (Spanish)	1994		Their Technical Measurement is ineffective.	
	Law 25,326 on the Protection of Personal Data (Spanish)			Cooperative Measures Are Weaker.	
	Decree 1558/2001 (Spanish)			They have a shaky judicial system for punishing offenders.	
	Provision 60 – E/2016 (Spanish)				
	Resolution 159/2018 - RESOL-2018-159-APN-AAIP (Spanish)				
	Agreement 108 approved by Law No. 27,483 (Spanish)				
Computer crime Statutes	Criminal Code of the Argentine Nation – Habeas Data Law 25326, year 2000 (Spanish)	2000			
	Law 26.388 (2008) (Spanish))				
	Law 27411, Agreement on Cybercrime (Spanish)				
	Criminal Code of the Argentine Nation (Spanish)				
	Law 26,388 of Law of Computer Crimes (Spanish)				

access and Accessibility) Act 1979 (the TIA Legislation), the Criminal Act 1995 (the Crimes Act), the Joint Assistance in Criminal Affairs Ordinance (the MA Act), as well as the Telecommunication Act 1997 (the Communications Act) to guarantee compliance with the European commission Convention on Cybercrime[3]. The Convention urges governments to work together to stop cybercrime by making it a requirement that countries ban four types of online crimes.

- Anomaly Criminal eavesdropping, information leakage, system interference, and device abuse are all examples of offences that jeopardize the availability, integrity, and confidentiality of computer information and services other offences include interception of data without authorization.
- Examples of offences that include the use of computers include forgery and fraud.
- Offences containing material, such as child pornography and
- Violating copyrights and committing comparable rights violations

Table 2. Categorization of Laws in Australia

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Electronic Transactions Act 1999, amended in 2011[19]	1999	To pursue violators, they adopt harsh legal procedures.	They have a less efficient Organizational Measurement.	12
Data Security and Privacy Regulations	Privacy Act 1988	1998	They have significant growth potential.	Their Technical Measurement is ineffective	
Computer crime Statutes	Criminal Code Act No. 12 of 1995 as amended in 2012[11]	1995	They use Cooperative Measures to combat criminals.		
	Cybercrime Legislation Amendment Act No.120/2012				

2.3 Brazil

On the ground, Brazilian law enforcement and military agencies are substantially investing in cyber-security. Despite this, there appears to be a mismatch between the sorts of threats that threaten Brazilian cyberspace and the style of security organization's reactions. Even though organized crime is one of the most serious dangers to Brazil's internet, the country's resources are disproportionately focused on military solutions that are better suited to the (very uncommon) situation of conventional conflict. Expanding day-to-day law enforcement skills to identify and respond to organized criminal organizations receives less attention. Brazil is adopting an imbalanced approach to cybersecurity due to a lack of a united government perspective on the problem and a lack of trustworthy data. Instead, a tiny group of powerful businesses and individuals are influencing the discussion in ways that will have a major impact on Brazil's cyber-security architecture in the future. The Unit for Combating Cybercrime (URCC) of the Federal Police is the primary law enforcement body in charge of preventing and responding to cybercrime. This responsibility falls under the umbrella of the Unit for Combating Cybercrime (URCC)[46] [39].

2.4 Canada

The federal government of Canada, based in the Parliament building in Ottawa, is responsible for making national laws, which are subsequently implemented across the country's 13 jurisdictions (ten provinces and three territories). The federal government of Canada, which is governed by the Criminal Code, is responsible for establishing (or repealing) new criminal laws. The provincial and territorial administrations are permitted to draught their laws, but these laws may only be enacted within their national borders. Provincial and territorial governments do not have the authority to enact new criminal laws, but they do have the authority to penalize those who violate provincial and territorial laws, such as by fining them or sending them to prisons [24].

Table 3. Categorization of Laws in Brazil

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Provisional Measure No. 2,200-2, of August 24, 2001, Establishes the Brazilian Public Key Infrastructure–ICP-Brazil and makes other provisions (Portuguese)[32]	2001	To pursue violators, they adopt harsh legal procedures.	They have a less efficient Organizational Measurement.	18
Data Security and Privacy Regulations	Protection of Personal Data Bill 2011	2014	They have significant growth potential.	Cooperative Measures Are Weaker.	
	Internet Act (Law No 12.965, April 23rd 2014). Articles 7 and 8			Their Technical Measurement is ineffective	
	General Data Privacy Law				
Computer crime Statutes	Penal Code Brazil	2008			
	Law No. 12,965, of April 23, 2014				
	Law 11,829/2008				
	Law No. 12,737, November 30th 2012				

In the latter half of 2014, the Protecting Canadians from Internet Crime Act was passed into law to bring both the Canadian Criminal Code and the Canada Evidence Act up to date. Police chiefs from throughout Canada have come out in support of the measure, stating that it will assist in the fight against online bullying and non-consensual sexting involving children and that it's time t stop those who harass, threaten, and fear them. The Safeguarding Canadians from Online Crime Act did add new Crimes Act infractions for disbursing and transferring a sexual image of a person without their permission and for recording, storing, and spreading child pornography. It also went after cyber espionage and telecommunications signal theft, just like its predecessor, Bill C-30[24] [41].

2.5 China

Cyber security was first considered at such a high level in President Hu Jintao's 2012 Work Report to the 18th CCP Congress. A strategy for China's cyber defence has not been made public. Despite this, it has implemented a variety of different data security procedures. The Chinese approach can be implemented above cyber security and incorporates the common aim of data security. Information security, defined by China, is "based on prior information systems and cybersecurity from unauthorized access, use, evaporation, damage, alteration, and ruination in store their integrity, secrecy, and availability." At the national level, a strategy paper would need to be released by President Xi Jinping or perhaps the Communist Party's Federal Congress, while policy papers are produced at the government level. To achieve this goal, the important announcements

Table 4. Categorization of Laws in Canada

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5[31]	2000	To pursue violators, they adopt harsh legal procedures.	Their Technical Measurement is ineffective.	8
Data Security and Privacy Regulations	Personal Information Protection and Electronic Documents Act	2000	They have effective organizational measures in place.	Cooperative Measures Are Weaker.	
Computer crime Statutes	Criminal Code of 1985[31]	1985	They have significant growth potential.		
	Evidence Act 2010[31]				

Table 5. Categorization of Laws in China

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Electronic Signatures Law of the People's Republic of China of 2004[18]	2004	They have significant growth potential.	They have a less efficient Organizational Measurement.	33
Data Security and Privacy Regulations	The Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection, 2012[28]	2012	To pursue violators, they adopt harsh legal procedures.	Their Technical Measurement is ineffective.	
	The Decision of the Standing Committee of the National People's Congress on Strengthening the Network Information Protection, 2012[14]		Cooperative Measures Are Weaker.		
Computer crime Statutes	Criminal Law as amended	1997			

made by President Xi have been used as a roadmap to direct the construction of policies implemented at the ministry level. The advancement of the country's information security industry is governed by the 12th Five-Year Transformation Programme of the Information Governance Sector (2011–15), which was publicly released by the Ministry of Industry Technology. This plan establishes goals and targets for the industry as well as regulates its growth. On the other hand, the report is much more of an industrialization program than a comprehensive plan for protecting sensitive information[36].

2.6 France

As France continues to expand its cyber capabilities, the ANSSI is increasing its ability to combat cyber threats. Furthermore, the cyber-security policy has emphasized crucial domains of action to achieve the strategic goals of the country,

Table 6. Categorization of Laws in France

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]]
Electronic Transaction Laws	Law No 2000-230 of March 13, 2000, adapts the law of the species to information technologies and relates to the electronic signature (French)[27]	2000	To pursue violators, they adopt harsh legal procedures.	They have a less efficient Organizational Measurement.	9
Data Security and Privacy Regulations	The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)[33] Law relating to the protection of individuals against the processing of personal data Law 78-17 of January 6, 1978, relating to data processing, files and modified freedoms (French)	1978	They have significant growth potential. To tackle criminals, they adopt Cooperative Measures.	Their Technical Measurement is ineffective.	
Computer crime Statutes	Law No. 2004-575 of June 21, 2004, for confidence in the digital economy (French)	2004			

exhibiting a thorough awareness of the issues that have been raised. In addition, the Cyber Defensive Alliance outlines several steps that will increase France's capacity to react to cyber-attacks. By the goals of the national cyber strategy, these activities have been intended to be implemented with the finances that are now available. As a part of the agreement, financial assistance for academic institutions and small and medium-sized businesses will be provided to foster research and innovation in the business sphere. First and foremost, it's important that France can protect its most important resources and national goals, even though the technology is changing quickly and there are many different ways to attack online[36][45].

Because of its substantial economic, technical, and intellectual skills in the sphere of cyberspace, France is a leading actor on the global stage. The current institutionalization process, in addition to supporting regulations and the Information Security Pact, has sped up the formation of French cyberspace security and cyber defence capabilities. This is the case even though political participation in the sector began at a very late stage[36][45].

2.7 Germany

Cybersecurity. Among the laws addressed are data security and e-privacy rules, forms of intellectual property Laws, client confidentiality Laws, data security requirements, and legitimate constraints. Several German laws govern cyber security. It is widely acknowledged that German Security Act is the most significant legal foundation for cybersecurity[45].

Additionally, there are several essential unwritten IT security principles in Germany. Minimum Baseline for Information Technology Security (BSI), Basic

Table 7. Categorization of Laws in Germany

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Law to adapt the formal requirements of private law to modern legal transactions (Federal Law Gazette I 2001 p. 1542)	2001	They use harsh legal measures to prosecute offenders.	They have a less efficient Organizational Measurement.	13
Data Security and Privacy Regulations	The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)[33]	2016	They took Technical Measurement.	Cooperative Measures Are Weaker.	
	Federal Data Protection Act[20]				
Computer crime Statutes	Network Enforcement Act, 2017[4]	2015			
	German Criminal Code 1986, as espect in 2015 para.202				

Guidelines for Cybersecurity Evaluation-2012, established as ISO/IEC 15408, and the objective for control of information and associated technology (COBIT) are all contained in this document[45].

2.8 India

The Legislation of 2000, which was modelled after the General Assembly Model The International Law produced the Law on Electronic Transactions Commission Maastricht Treaty (UNCITRAL), is India's major computer crime and e-commerce statute. Originally, the Act was divided into 94 parts including 13 sections and a total of four schedules. The Act is applicable across the whole of India., as well as actions or breaches done by anybody, regardless of nationality, beyond India's borders. The Act grants electronic records legal power and greatly simplifies the remote filing of documents with government agencies[25].

The Information Technology Act of 2000 has four main objectives:

- To guarantee legal recognition of digital records
- To enable the official status of digital signatures. Traditional signatures are vulnerable to fabrication and alteration, making them unfit for use in online transactions and contracts. Digital signatures provide the unique and powerful protection those online transactions demand
- To give electronic administration legal status. The phrase e-governance refers to a technology-driven government that uses technology to offer services, information, and education more efficiently
- To impose penalties for cybercrime. The Indian Penal Code of 1860 was insufficient to address the rising threat of cybercrime. These offences were both unique and high-tech, necessitating a new category under the Information Technology Act of 2000[25]

Table 8. Categorization of Laws in India

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Information Technology Act 2000[25]	2000	To pursue violators, they adopt harsh legal procedures.	They have a less efficient Organizational Measurement.	10
Data Security and Privacy Regulations	Bill – Personal Data Protection, 2019[34]	2000	They have significant growth potential.	Their Technical Measurement is ineffective.	
	Information Technology Act 2000[25]		To tackle criminals, they adopt Cooperative Measures.		
Computer crime Statutes	The Information Telecommunication Act of 2000, amended in 2008 – ITA	2000			

Table 9. Categorization of Laws in Indonesia

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions[42]	2008	To tackle criminals, they adopt Cooperative Measures.	They have a less efficient Organizational Measurement.	24
Data Security and Privacy Regulations	Systems Regulation 2016[42]	2016	They have significant growth potential.	Their Technical Measurement is ineffective.	
Computer crime Statutes	Law of the Republic of Indonesia Number 11 of 2008 Concerning Electronic Information and Transactions[42]	2008		They have a shaky judicial system for punishing offenders.	

2.9 Indonesia

When it comes to ensuring the safety of its computer networks, Indonesia already has a framework and policy in place, both of which are carried out by various government agencies as well as by the general population. The Cabinet of Communication and Information Technology is responsible for cyber security policy (MCI). Three government entities in Indonesia are involved in the field of cyber security. These organisations include the Information Security Coordinating Team and the Director of Indonesia Security Operations Team on Internet Connections and Information Security (ID-SIRTII)[48].

In April 2010, the Internet Security Interoperability Team was created to coordinate computer security, with a focus on technology and information competency and practices. The Director of Information Security is important for policy creation and implementation, education, surveillance, evaluation, and reporting in the area of data security governance. Depending on the Ministry of Communications and Informatics Regulatory Oversight No. 8 of 2012, the government established ID-SIRTII to oversee the security of internet infrastructure[48].

Table 10. Categorization of Laws in Italy

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	DLegislative Decree 7 March 2005, n. 82 Digital Administration Code - updated to the expected decree of 13 December 2017, nr. 217 (Italian)	2005	To pursue violators, they adopt harsh legal procedures.	Their Technical Measurement is ineffective.	20
Data Security and Privacy Regulations	Data Protection Code Decree No. 196/2003 The General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR)[33] Legislative Decree 30 June 2003, n. 196 - Code regarding the protection of personal data (Italian)	2003	They have significant growth potential. They have effective organizational measures in place.	Cooperative Measures Are Weaker.	
Computer crime Statutes	Penal Code. (Italian)[10]	2009			

2.10 Italy

The introduction of the internet in the middle of the 1990s led to an increase in the Italian police's understanding of cybercrime, which in turn caused them to grow concerned about issues related to cyber security. A unit for telecommunications was founded in 1996, and two years later, in 1998, the Postal and Communications Police Service came into being. A task force was established by the Financial and Border Police (Guardia di Finanza) in the year 2001[38].

In 2010, the House National Council on Intelligence and Security Service of the Italian government issued the first formal public assessment of Italy's national cyber security problems. This study was commissioned by the Italian government. The concept of asymmetric cyber threats was put up in the paper, which also described cyberspace as the "new battlefield" of the 21st century and the "scenario of geopolitical conflict." The report focused on four primary concerns: Cyber-crime, cyberterrorism, cyberespionage, and cyber-warfare are all examples of cybercrime. According to the study's findings, Cyber security is a strategic problem as well as a threat to public safety[36]. One of Italy's strengths in terms of its cyber security policy is the presence of police systems specifically designed to fight cybercrime. The enforcement of copyright laws, as well as Child pornography on the internet, computer hacking, malware, and fraudulent E-commerce transactions, are the primary areas of concentration for the activities of the Postal and Communications Police Service. Fraud committed through digital means is the primary target of the Guardia di Finanza task force. The Carabinieri have both a cybercrime special investigative branch and a piece of information and communications technology security section[36].

Table 11. Categorization of Laws in Japan

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Law Concerning Electronic Signatures and Certification Services, Law No. 102 of 2000	2000	To pursue violators, they adopt harsh legal procedures	They have a less effective Organizational Measure.	7
Data Security and Privacy Regulations	Act on the Protection of Personal Information[2]	2003	They have significant growth potential.		
Computer crime Statutes	Unauthorized Computer Access Law, 2013	1999	To tackle criminals, they adopt Cooperative Measures.		
	Penal Code		They took Technical Measurement.		

2.11 Japan

Japan ranked fourth among the countries of the Asia Pacific territory relative to the number of people who use the internet in January 2021, with over 117 million them. Security concerns have emerged as one of Japan's most pressing internal challenges as a direct result of the growing significance of digitalization to the country's economy and the people's day-to-day lives. In 1973, the Tokyo District Court was the venue for the hearing of Japan's first case involving a criminal offence employing a computer. This wasn't a criminal case; rather, it was a civil dispute between two parties. However, the theft of data was the primary worry in this instance. Nikkei Shimbun, which is a well-known news organization in Japan, and McGraw-Hill at the time established Nikkei McGraw-Hill. The plaintiff was awarded 2,039,420 Japanese Yen in damages, and the defendant was ordered by the Tokyo District Court to pay a portion of the plaintiff's expenditures and damages[36]

It is now criminal in Japan under the Cybersecurity Act to access the system without authorization. This Law aims to avoid computer-related crimes committed via telecommunication links and to maintain telecommunications network order, as realized through physical access features, by restricting acts of unauthorized computer access and specifying penalties for that acts, as well as additional Encourage regional public safety commissioners to implement preventative steps to reduce the likelihood of similar incidents happening in the future and hence making contributions to the better and healthier development of the nation. This Act was passed to accomplish these goals[36].

2.12 South Korea

The incidence of cyber-attacks has risen, and the society of the Republic of Korea is now susceptible to the threats posed by the Democratic People's Republic of Korea. This is because computer networks and information systems play such a

Table 12. Categorization of Laws in South Korea

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Digital Signature Act No. 5792/1999[26]	1999	To pursue violators, they adopt harsh legal procedures.	They have a less effective Organizational Measure.	4
Data Security and Privacy Regulations	Personal Information Protection Act	2020	They have significant growth potential.		
Computer crime Statutes	Act on the protection of information and communication Infrastructure	2016	To tackle criminals, they adopt Cooperative Measures.		
	Act on Promotion of Information and Communications Network Utilization and Information Protection		They took Technical Measurement.		

significant role in the day-to-day lives of people. Legislation and national strategies that are up to par are required to effectively respond to internal and external cyber-attacks. As part of the Republic of Korea's ongoing efforts to protect the nation, several laws and regulations have been enacted as a direct result of these efforts[40].

In 2002, the Republic of Korea's government passed the Critical Information Infrastructure Protection Act, emphasizing the need of protecting as a matter of national security, critical data infrastructure must be protected from cyber-attacks. This law has been in effect ever since. To defend CII from cyberattacks, the Act mandated the creation of a national agency and imposed rules on CII designation, vulnerability assessment and protection measures, cyber incident response, and punishments[40].

In addition, to enhance the nation's overall cyber security, Korean policy-makers and legislators have recently held several hearings, and they have also passed the Cyber Security Industry Enhancement Act. This Act gives Central and local administrations in Korea, as well as municipalities, the ability that devise and carry out policies that promote cyber security, as well as prepare measures to allocate budgets to support those policies[40].

Members of the National Assembly proposed a measure that would solely focus on the security of personal information. The proposal was approved on March 29, 2011, and the Act has been in effect since September 30, 2011. The Act addresses the obligations that must be fulfilled by managers of personal information and relevant ministers of the government[40].

2.13 Mexico

The Mexican Working Group on Combating Cybercrime (CERT-MX) and the Electronic Digital Signature act were both made. Also, Cybersecurity Standards were made, but you don't have to use any of the official certification methods.

Table 13. Categorization of Laws in Mexico

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Advanced Electronic Signature Law (Spanish)[5]	2012	They have significant growth potential.	They have a less efficient Organizational Measurement.	52
Data Security and Privacy Regulations	General Law on the Protection of Personal Data held by obligated subjects (Spanish)	2010		Their Technical Measurement is ineffective.	
	Federal Law on the Protection of Personal Data Held by Private Parties 2010 (Spanish)			Cooperative Measures Are Weaker.	
	Agreement for the Protection of Persons concerning the Automated Processing of Personal Data and Additional Protocol to the Agreement for the Protection of Persons concerning the Automated Processing of Personal Data, Control Authorities and Transborder Data Flows (Promulgatery Decree) (Spanish)			They have a shaky judicial system for punishing offenders.	
	General Guidelines for the Protection of Personal Data for the Public Sector (Spanish) Regulation Federal Law on Protection of Personal Data Held by Private Parties (Spanish)				
	General Law of Transparency and Access to Public Information (Spanish)				
	Federal Law of Transparency and Access to Public Information (Spanish)				
Computer crime Statutes	Federal Penal Code (Spanish)	2020			

This could be because the government doesn't want to "over-regulate" the cybersecurity business. The National Information Security Strategy of Mexico was made by a committee on special information security. This plan was put in place by Mexico (CESI). In official papers in Mexico, the word "cybersecurity" appears sparingly, although the term "information security" appears often. The police force in Mexico is in charge of the cybersecurity of the country. Mexico's role in international cooperation is limited to its commitment to the United Nations and the Organization of American States' fight against cyber-terrorism and cyber-crime[37].

2.14 Russia

Most of Russia's laws about data protection and privacy were passed in 2005 and 2006, so this area of the country's legal code is growing quickly. The Russian Fed-

eral Data Protection Law (No. 152-FZ), which went into effect on July 27, 2006, serves as the cornerstone of Russian privacy laws, and data controllers are obligated to adopt “all essential organizational and technological measures needed for securing personal data from unauthorized or accidental access." The Federal Service for the Supervision of Communication, Information and Technology, and Mainstream Media makes sure that everyone is following the rules[40].

Individuals are generally expected to provide their consent before their data is processed; however, this regulation does not apply in cases where the customer is a signatory to an agreement that requires the processing of their personal Federal Service on Telecommunications, which is responsible for data protection and privacy, has declared in the past that appropriate protection only exists among foreign jurisdictions where the Agreement for the Protection of Individuals Regarding Automatic Processing of Private Information has been signed and ratified. However, three key exclusions enable private data to be sent to nations with a lower level of personal data protection or with no obligation at all. On September 1, 2015, a new clause referred to as “Article 18(5)" comes into force, imposing further restrictions on the transmission of data[36].

In Russia, direct marketing, data processing and management of all data are subject to stringent regulations. Personal data must be adequately protected by applicable laws and the Federal Security Service is currently in the process of formulating required data protection regulations. The regulations mandate the use of encryption to protect any personally identifiable information that is sent outside of Russia, and it is expected that only Russian encrypted software and hardware would be used [47].

2.15 Saudi Arabia

The number of instances of cybercrime has been steadily increasing all over the world. As a direct consequence of this, ensuring cyber security is essential. It is critical to have adequate technological procedures for cyber-security in place. Nevertheless, the establishment of a legislative structure that allows for cyber-security is also a crucial component. Every nation’s governing body should enact basic criminal legislation to combat cybercrime to boost the level of trust and confidence that users have in cyberspace[35].

The Saudi Arabian Anti-Cyber Crime Law was finally approved in March of 2007. (ACC). According to the ACCL, unauthorized access is defined as any person’s deliberate computer access, internet sites, data management, and computer networks that are not permitted by the owner of such resources. This legislation provides both a definition of what it means to commit a crime online as well as the accompanying punishments for doing so. The Saudi ACCL has all of the essential qualities critical to safeguarding the network’s integrity Despite this, there are still several areas in which the Saudi ACCL has room for improvement to become more successful[35].

Table 14. Categorization of Laws in Russia

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Federal Law No. 476- on Electronic Signatures and protection of the rights of legal entities and individual entrepreneurs (Russian)	2019	To pursue violators, they adopt harsh legal procedures.	They have a less effective Organizational Measure.	5
Data Security and Privacy Regulations	Bill – Regarding Personal Data[21]	2006	They have significant growth potential.	Their Technical Measurement is ineffective.	
	Federal law No. 152-FZ of 27 July 2006 "On Personal Data" (with the latest amendments of 2 July 2021)		To tackle criminals, they adopt Cooperative Measures.		
Computer crime Statutes	Federal Law No. 187-FZ of 26 July 2017[29]	2006			
	Criminal Code of the Russian Federation (with the latest amendments of 1 July 2021), Chapter 28. Crimes in the Sphere of Computer Information				
	Federal Law No. 149-FZ of 27 July 2006 "On Information, Information Technologies, and Protection of Information" (with the latest amendments of 2 July 2021)				

2.16 South Africa

Particular cybercrime law has been enacted in South Africa, and it goes under the name of the Electronic Communications and Transaction Act [17], By Chapter 13 of this Act, the followibehavioursors are considered unlawful: The first clause of Section 86(1) makes it illegal to intercept or access information without authorization.

- Unauthorized willful interference with information that results in the information's change, ineffectiveness, or destruction is a violation of section 86(2) of the Computer Fraud and Abuse Act.
- (Articles 86(3) and 86(4)): Avoiding security safeguards by any means, such as advertising, spreading, or owning a gadget designed to do just that.
- An attack that results in a whole or partial denial of service is considered to violate Section 86(5).
- (Section 87): Theft, fraud, and counterfeiting that include the use of computers.
- Attempting any of the conduct listed above, as well as helping and abetting in any of the activities listed above, is a violation of Section 88 of the Criminal Code[17].

2.17 Turkey

In October of 2010, the Information and Communication Technologies Authority advised providers of telecommunications services to conform with the standards

Table 15. Categorization of Laws in Saudi Arabia

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Electronic Transactions Law No. 18 of 2007	2007	To pursue violators, they adopt harsh legal procedures.	Their Technical Measurement is ineffective.	2
Data Security and Privacy Regulations	Personal Data Protection Law (PDPL)	2022	They have significant growth potential.		
Computer crime Statutes	Anti-Cybercrime Law 1428/2007[6]	2007	To tackle criminals, they adopt Cooperative Measures. They have effective organizational measures in place.		

Table 16. Categorization of Laws in South Africa

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Electronic Communications and Transactions Act, updated in 2010[15]	2010	They have significant growth potential.	They have a less efficient Organizational Measurement.	59
Data Security and Privacy Regulations	Protection of Personal Information Act 4 of 2013	2013		Their Technical Measurement is ineffective.	
Computer crime Statutes	Electronic Transactions and Communications Act 2002[17]	2002		Cooperative Measures Are Weaker. They have a shaky judicial system for punishing offenders.	

established by ISO 27001. In July of 2014, the regulatory body established a new, stricter criterion for determining compliance with ISO 27001. (ICTA, 2014). The Telecommunications and Computer Security in the Communications Sector Act specifies the requirements for security countermeasures and information system attributes, as well as the external and internal audit mechanisms that must be implemented by operators[44].

The Banking Regulation and Supervision Agency have been responsible for the creation of several pieces of financial legislation. In January of 2008, the BSRA published a legal announcement about the management of bank information security. The announcement includes a variety of measures, including Management of information security risks, management responsibility, internal audit, outsourcing regulations, function separation, and other issues (BRSA, 2007), (BRSA, 2010)[44]. Just one more piece of law lays forth the standards for independent external auditors to follow while conducting assessments of banks' information systems.

Table 17. Categorization of Laws in Turkey

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]]
Electronic Transaction Laws	Law 5070/2004 Electronic signature	2004	To pursue violators, they adopt harsh legal procedures.	They have a less efficient Organizational Measurement.	11
Data Security and Privacy Regulations	Law on the Protection of Personal Data No. 6698, 2016[1]	2016	They have significant growth potential.		
Computer crime Statutes	Turkish Criminal Law	2004	To tackle criminals, they adopt Cooperative Measures. They took Technical Measurement.		

In February of 2014, the Electronic Communications Law went through a round of revisions to reflect decisions taken by the cabinet in October of 2012. (Turkish Cabinet, 2014) As a direct effect of these many adjustments:

- ECL was tasked with putting together the Cyber Resilience Council from the ground up. The leader of the Cyber Defense Commission is the Minister of Transport, Maritime Affairs, and the Cyber Security Interim president. For example, one task that fell under the council's purview was to provide final approval to a list of important infrastructure.
- An explanation of the Transportation Ministry, Communications Ministry and Maritime Affairs' cyber security responsibilities were provided. Identifying vital infrastructures, as well as their owners and the locations of such infrastructures, was one of the ministry's objectives.

2.18 United Kingdom

In the year 2000, the Electronic Communications Act was passed into law by the legislature of the United Kingdom. Encryption, encrypted communication services, and electronic signatures are some of the growing trends that were targeted by the act, which was passed to help with the monitoring and supervision of new trends in the eCommerce industry[8].

To ensure the legitimacy of electronic signatures and to regulate cryptographic services within the United Kingdom, a law was required to be developed and passed into law. The Electronic Communications Act of the United Kingdom is broken up into three distinct sections, each of which provides regulations and protections about a different facet of the subject matter that is detailed further below

The First Section: Cryptographic Service Providers. E-commerce and the convenience of data storage are covered in Part 2. (Which is inclusive of eSignatures). The third section will include supplementary and other items

Table 18. Categorization of Laws in United Kingdom

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	Electronic Communications Act 2000[16]	2000	To pursue violators, they adopt harsh legal procedures.	Their Technical Measurement is somewhere ineffective.	2
Data Security and Privacy Regulations	Data Protection Act 1998[12]	1998	They have significant growth potential.		
	Data Protection Act 2018[13]		To tackle criminals, they adopt Cooperative Measures.		
Computer crime Statutes	The Computer Misuse Act of 1990, as amended[9]	1990	They have effective organizational measures in place.		

Laws such as the United Kingdom Electronic Communications Act (2000) and the Electronic Signatures Ordinance of 2002 encourage and support robust e-Commerce activity for businesses while also improving the security and legitimacy of these forms of digital payments for customers[8].

2.19 United State of America

The United States of America was the world's first nation to pass legislation specifically addressing data privacy, which was known as "The Privacy Act of 1974." Information from a monitoring system can't be released without the explicit agreement of the individual in question, according to the Privacy Act. unless the disclosure falls under one of twelve statutes about the subject material of the record. The relevance of revising laws governing cyber security is closely tied to digital change, cybercrime, and the investigation of cyber forensics. An integrated digital cyber legal system is required for a movement toward tech-centric smart cities and cyber-confident citizenship. Without such a system, the process of establishing the digital transformation and environment may become more disjointed. "Technology removes the need for, and indeed the ability to focus on specific, localized activity." This results in a new 2 The network is a type of social organization that is arranged in a physical domain."Physical constraints, proximity, patterns, and scale are all important characteristics of verifiable wrongdoing. "Communication technologies liberate us from the constraints of the empirical world; we can communicate with anyone, from anywhere, in real-time." Technology removes the need for, and It is not required that the victim and the perpetrator be located near one another. "Because cybercrime is an unbounded crime, the victim and the perpetrator can be in different cities"[30]. "Cybercrime is a crime with no physical boundaries."

Table 19. Categorization of Laws in United State

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	EElectronic Signatures in Global and National Commerce Act (E-SIGN), 15 U.S.C. 7001-7003	1996	To pursue violators, they adopt harsh legal procedures.		1
Data Security and Privacy Regulations	Privacy Act of 1974[12]	1974	They have significant growth potential.		
	Federal Trade Commission Act 15[22]		To tackle criminals, they adopt Cooperative Measures.		
Computer crime Statutes	Computer Fraud and Abuse Act 1986[7]	1986	They have effective organizational measures in place.		
	Title 18 – Crimes and Criminal Procedure		They took Technical Measurement.		

Table 20. Categorization of Laws in European Union

Law Type	Act Name	Introduce year	Laws Pros	Laws Cons	Global Ranking[23]
Electronic Transaction Laws	on electronic identification and trust services for electronic transactions in the internal market	2014	To pursue violators, they adopt harsh legal procedures.	They have a less efficient Organizational Measurement.	-
Data Security and Privacy Regulations	General Data Protection Regulation Act[33]	2016	They have significant growth potential.		
Computer crime Statutes	EU Cybersecurity Act	2019	To tackle criminals, they adopt Cooperative Measures.		
			They took Technical Measurement.		

2.20 European Union

The Network and Information Security Agenda in 2001, the very first e-Privacy Guideline in 2002, the setup of ENISA in 2004, the Critical Information Infrastructure Information exchange in 2009, the Digital Ideology for Europe in 2010 and the EU Cybersecurity Strategy in 2013. All of these steps were taken by the European Commission. However, to what extent did it exert its influence? We have raised awareness between many elected figures, industry Chief executives, and the Computer Emergency Responders team in each of our 28 member countries. The majority of member states have already developed comprehensive national cybersecurity strategies. However, there is no comprehensive European Union policy document for network and data security. This system would need to include full event reporting (similar to what is done in the telecoms sector), as well as trustworthy communication about risks and attacks. Under NIS policy, which is designed to address these issues and is now the subject of negotiations between the European Council and the Parliament, which is currently under

construction. The fact that cyber-security is widely regarded as a component of national security, and consequently comes within the purview of national sovereignty, continues to be a barrier to progress. As a consequence of this, there is still a significant distance to go before Europe will have cyberspace that is both open and safe.

3 Conclusions

In this paper, We have analyzed the various laws of the G20 countries. We have identified their associated pros and cons and briefly summarized them. The article also presents a comparative study between them and suggests how the individual G20 country makes their decision by applying associated laws for a particular issue.

References

1. About legislation preparation procedures and principles regulation. https://www.mevzuat.gov.tr
2. Act on the protection of personal information act no. 57 of (2003). https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf
3. An act to implement the council of europe convention on cybercrime, and for other purposes. http://www.comlaw.gov.au/
4. Act to improve enforcement of the law in social networks (network enforcement act). https://www.bmj.de/SharedDocs
5. Advanced electronic signature law. https://www.diputados.gob.mx/LeyesBiblio
6. Anti-cyber crime law. https://wipolex-res.wipo.int/edocs/lexdocs/laws
7. Computer fraud and abuse act. http://cio.doe.gov/Documents/CFA.HTM
8. Computer misuse act. https://www.cps.gov.uk/legal-guidance/computer-misuse-act
9. Computer misuse act 1990. https://www.legislation.gov.uk/ukpga/1990/18/contents
10. Crimes against public faith. https://www.brocardi.it/codice-penale/libro-secondo/titolo-vii/
11. Criminal code act 1995. https://www.legislation.gov.au/Details/C2017C00235
12. Data protection act 1998. https://www.legislation.gov.uk/ukpga/1998/29/contents
13. Data protection act 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents
14. Decision of the national people's congress on strengthening the network information protection. http://www.gov.cn/jrzg
15. e-government services. https://www.eservices.gov.za/
16. Electronic communications act 2000. https://www.legislation.gov.uk/ukpga/2000
17. Electronic communications and transactions act 25 of 2002. https://www.gov.za/documents/electronic-communications-and-transactions-act
18. Electronic signature law of the people's republic of china. http://www.npc.gov.cn/zgrdw/englishnpc/Law
19. Electronic transactions act 1999. https://www.legislation.gov.au/Details
20. Federal data protection act (bdsg). https://www.gesetze-im-internet.de

21. Federal law of the russian federation. https://cis-legislation.com
22. Federal trade commission act. https://www.ftc.gov/legal-library
23. Global cybersecurity index 2020. https://www.itu.int/en/ITU-D/Cybersecurity
24. International cybercrime research centre, simon fraser university. https://www.sfu.ca/iccrc.html
25. It act, 2000. https://www.meity.gov.in/content/information-technology-act-2000
26. Korean law information center. https://www.law.go.kr
27. Law no. 2000-230. https://www.legifrance.gouv.fr
28. National people's congress standing committee decision concerning strengthening network information protection. https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/
29. On the security of the critical information infrastructure of the russian federation. http://pravo.gov.ru/proxy/ips
30. Overview of the privacy act: 2020 edition. https://www.justice.gov/opcl
31. Prescribed information for the description of a designated project regulations. https://laws-lois.justice.gc.ca/pdf/SOR-2012-148.pdf
32. Provisional measure no. 2.200-2 , of august 24, 2001. http://www.planalto.gov.br
33. Regulation (eu) 2016/679 of the european parliament. http://data.europa.eu/eli/reg
34. The personal data protection bill, 2019. http://164.100.47.4/BillsTexts/LSBillTexts
35. Alshammari, T.S., Singh, H.P.: Preparedness of saudi arabia to defend against cyber crimes: An assessment with reference to anti-cyber crime law and gci index. Archives of Business Research **6**(12) (2018)
36. Baylon, C.: Challenges at the intersection of cyber security and space security: country and international institution perspectives (2014)
37. Bolgov, R.: The un and cybersecurity policy of latin american countries. In: 2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG). pp. 259–263. IEEE (2020)
38. De Zan, T., Giacomello, G., Martino, L.: Italy's cyber security architecture and critical infrastructure. In: Routledge Companion to Global Cyber-Security Strategy, pp. 121–131. Routledge (2021)
39. Diniz, G., Muggah, R., Glenny, M.: Deconstructing cyber security in brazil. Strategic Paper (2014)
40. Eom, Y.J., Ivanov, A.M.: A comparative analysis on cyber security law between republic of korea and russian federation. . . (1 (13)), 69–79 (2020)
41. Huey, L., Ferguson, L.: Cyberpolicing in canada: A scoping review (2022)
42. ITE, U.: The law of the republic of indonesia number 11 of 2008 concerning electronic information and transactions (2008)
43. Kapila, P.: Cyber crimes and cyber laws in india: An overview. Contemporary Issues and Challenges in the
44. Karabacak, B., Yildirim, S.O., Baykal, N.: Regulatory approaches for cyber security of critical infrastructures: The case of turkey. Computer law & security review **32**(3), 526–539 (2016)
45. Kavyn, S., Bratsuk, I., Lytvynenko, A.: Regulatory and legal enforcement of cyber security in countries of the european union: The experience of germany and france. Teisė **121**, 135–147 (2021)
46. Kshetri, N.: Cybersecurity in brazil. In: The Quest to Cyber Superiority, pp. 195–209. Springer (2016)

47. Kshetri, N.: Cybersecurity in russia. In: The Quest to Cyber Superiority, pp. 211–221. Springer (2016)
48. Rizal, M., Yani, Y.: Cybersecurity policy and its implementation in indonesia. Journal of ASEAN Studies **4**(1), 61–78 (2016)